IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF THE VEHICLE DESCRIBED AS A 2018 FORD TRANSIT CONNECT 4DR XLT, VIN NM0LS7E79J1368515, FURTHER DESCRIBED IN ATTACHMENT A	Case No. 3:21-sw-121

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Matthew Marasco, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a 2018 Ford Transit Connect 4DR XLT, VIN NM0LS7E79J1368515 (hereinafter referred to as "VEHICLE"), as further described in Attachment A, and for the seizure from the VEHICLE of items as further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been since September 2019. I am assigned to the Richmond Field Office of the FBI in Richmond, Virginia, and am responsible for conducting investigations pertaining to child exploitation. As part of my duties, I have received training regarding the investigation of Federal crimes including, but not limited to, crimes against children, human trafficking, civil rights, and public corruption. By virtue of my employment with the FBI, I have performed a variety of investigative tasks including conducting arrests and executing Federal search warrants. As a Special Agent, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. § 2422(b), Attempted Coercion and Enticement of a Minor, and 18 U.S.C. § 2423(b), Travel with Intent to Engage in Illicit Sexual Conduct, are located on the VEHICLE described in Attachment A. There is also probable cause to search the VEHICLE described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a courtof competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is "a district court of the United States … that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

6. **Coercion and Enticement**: 18 U.S.C. § 2422(b) provides that whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be imprisoned not less than 10 years or for life.

7. **Travel with Intent to Engage in Illicit Sexual Conduct:** 18 U.S.C. § 2423(b) A person who travels in interstate commerce or travels into the United States, or a United States

citizen or an alien admitted for permanent residence in the United States who travels in foreign commerce, with a motivating purpose of engaging in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. "**Computer**," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. "**Computer Server**" or "**Server**," as used herein is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

c. "**Computer hardware**," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and

diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. **"Computer software,"** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. **Wireless telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

f. **Digital camera**: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and

removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

g. **Portable media player**: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

h. **GPS**: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that

antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

i. **PDA**: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

j. **Tablet**: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

k. The "**Internet**" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "**Internet Service Providers**" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. "**Internet Protocol address**" or "IP address" refers to a unique number used by a computer to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

n. "The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade

form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

9. As described above and in Attachment B, this application seeks permission to search for records that might be found on electronic devices including cellular phones, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

10. *Probable cause.* I submit that there is probable cause to believe records will be stored on electronic devices including cellular phones, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a

storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

11. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers

were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the electronic devices including cell phones because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

12. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices including cellular phones consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

PROBABLE CAUSE

14. As part of an undercover operation conducted by the FBI Richmond Child Exploitation Task Force (CETF), an online covert employee (OCE) used a covert social media account to target subjects willing to travel to the Richmond, Virginia area to engage in sexual conduct with a minor. The OCE set up a profile posing as an adult intermediary who had access to both an 8-year-old male son and a 10-year-old female daughter. The OCE posted a profile on an online platform and subsequently responded to subjects who indicated a desire to meet with the minors.

15. The OCE posted an undercover (UC) profile on Alt.com, an online network for members interested in alternative forms of sexual relationships and friendship. Users can bond over fetishes, kinks, and BDSM (Bondage, Discipline, Sadism, and Masochism), as well as explore the site's large stockpile of sexual videos, articles, and other content. The UC profile noted that the user was an adult female from Chesterfield, Virginia. It also included a list of kinks to include "young/old," "bestiality," and "taboo family".

16. On June 21, 2021, an individual utilizing the username FL_Firmhand contacted the OCE through the UC profile on Alt.com (hereinafter referred to as "UC Mom" to protect the integrity of the OCE online profile). FL_Firmhand initiated the conversation by saying: "Your listed kinks is very interesting, You have the family, do you have the pet? My profile is open to standard members. Mike." FL-Firmhand's Alt.com provide stated he is a 61-year-old male from Opp, Alabama and contained several profile pictures what appeared to be a white, middle-aged male.

17. The conversation between FL_Firmhand and UC Mom continued on Alt.com for several days. During the conversation, FL_Firmhand stated he is interested in various sexual activities including, but not limited to, the use of sex toys and restraints, bestiality, and "more extreme things" which FL_Firmhand did not elaborate on. FL_Firmhand sent UC Mom a picture of his drivers license which identified him as MICHAEL KEVIN SMITH, date of birth July 22, 1959, with an Opp, Alabama address. The picture on the drivers license appeared to match the profile pictures on FL_Firmhand's Alt profile. SMITH also sent a picture of what appeared to be various sex toys and stated, "you asked about the toy bag. Here it is without a couple of more extreme things like a six strand hand whip and the needles that I did not figure would interest you [emoji]."

18. On June 28, 2021, FL_Firmhand asked to chat with UC Mom on Kik, provided the Kik username wyzardmike, and stated that he sent UC Mom a Kik message. On the same day, UC Mom received a message on Kik from an individual with the username wyzardmike and a vanity name of Mike Smith. SMITH inquired about the ages of UC Mom's children, and stated his children are grown now.

19. The conversation between SMITH and UC Mom continued on Kik, and on June 29, 2021, the following exchange occurred in reference to the SMITH's interest in engaging in sex with minors:

UC Mom - You mentioned being into age play
What have you done in that regard?

SMITH – Nothing under 16 at this point

UC Mom - Ok

SMITH – Not that I'm opposed
It's been more about what opportunities presented themselves

20. Later in the conversation, SMITH discussed engaging in sex with UC Mom and UC Mom's 10-year-old daughter (hereinafter referred to as "UC Daughter" to protect the integrity of the OCE online profile). SMITH also suggested he and UC Mom look for a dog to engage in sex with UC Mom and UC Daughter:

UC Mom – I would imagine when it gets to that point she'd need a smaller dog

SMITH – That would be a very good idea the dog could lick her

UC Mom – She'd probably love that
She absolutely loves oral

SMITH – If she sees a dog licking you liking it she will want to try it
Her and I will get along fine because I love licking p****

21. On July 1, 2021, SMITH agreed to chat with UC Mom on Whatsapp and provided the number 850-619-4628. Later that same day, UC Mom sent a Whatsapp message to the number provided by SMITH. The profile picture associated with Whatsapp user 850-619-4628 appeared to match one of SMITH's Alt profile pictures. SMITH and UC Mom exchanged the following messages:

UC Mom – Hi Mike, it's UC Mom
Or do you prefer Michael?

SMITH – Mike is fine Dear
How was your day?

22. The conversation between SMITH and UC Mom continued on Whatsapp and included exchanges about topics including, but not limited to, traveling to Richmond, Virginia and engaging in sex with UC Mom, UC Daughter, and UC Mom's 8-year-old son (hereinafter referred to as "UC Son" to protect the integrity of the OCE online profile), bestiality, bondage, and bringing various sex toys to use with UC Mom, UC Daughter, and UC Son. The following is an example of the conversation:

UC Mom – How was your day?

SMITH – Quiet
Sat around fantasizing

UC Mom – What were you imagining?

SMITH – You kneeling between my legs with UC Daughter and UC Son on either side as you explained what you were doing

UC Mom – That's a very doable thing

SMITH – Oral sex 101
This is precum see how slippery it is go ahead and feel
I think it is a scenario that we will all enjoy

Additionally, during the chats SMITH sent UC Mom a picture of what appeared to be a white male's penis and later asked UC Mom to show UC Daughter the picture.

23. On July 5, 2021, the following exchange occurred in reference to SMITH engaging in sexual activity with UC Daughter when he first traveled to Richmond, Virginia:

SMITH – If we don't go too fast so she should get sore then I would say probably I have toys that are about the same size as me that we can work with
I know you're looking forward to being there with her when she is with a man for the first time

UC Mom – I'll have to let her know not to expect sex the first visit then

SMITH – If I'm there for 5 days we could probably work and do it in that length of time
I'll use my finger and tongue to loosen her up some and my other toys
I just want to make sure that I don't hurt her

24. Later that same day, SMITH discussed engaging in sexual activity with UC Son:

SMITH – I try to run scenarios through my mind of ways that we can involve UC Son

UC Mom – How have you been thinking to work him in?

SMITH – I'm not sure what he's capable of so it's hard to figure out right now I don't know how big he is if he's able to penetrate or if you just suck him and he licks you or what
I figure I will teach him about erogenous zones and things that he can do to make a woman happy and excited so that when the times comes that he's ready for full sex he will have a better idea.

25. On July 12, 2021, SMITH spoke directly to UC Daughter via UC Mom's Whatsapp account. During the conversation, SMITH instructed UC Daughter to perform sex acts on UC Mom, and talked with UC daughter about engaging in sex with her when SMITH travels to Richmond, Virginia. The following is an example of the conversation:

SMITH – Did your mama tell you I have a fat tongue

UC Daughter – I like honey to
She showed me
It's reallly big

SMITH – What would you like me to do with it

UC Daughter – I wanna b licked

SMITH – How about if I lick you while you lick your mom

UC Daughter – Mom is really good at it n UC Son is ok

SMITH – Would you like that

UC Daughter – Ya I would tgat

SMITH – Then that is something we will have to do and then I can lick your mama while she licks you

Later in the same conversation, SMITH stated, "If I come inside your mom you can lick it out of her I think she would really like that".

26. The conversation between SMITH and UC Mom continued on Whatsapp and included discussion about SMITH driving to Richmond, Virginia from his residence in Alabama on July 28, 2021 to meet UC Mom, UC Daughter, and UC Son. SMITH stated he would be driving a van, discussed potential routes he may take, and stated the drive would be approximately 12 to 13 hours. SMITH also stated he would bring various sex toys including blindfolds and a vibrator.

27. Investigators used personally identifiable information from FL_Firmhand's Alt.com profile, information volunteered during the chat sessions on Alt, Kik, and Whatsapp, and information obtained from various open source and FBI database queries to identify SMITH as MICHAEL KEVIN SMITH, date of birth (DOB) July 22, 1959, social security number XXX-XX-2064, residing in Opp, Alabama. The list of vehicles registered to SMITH included the VEHICLE.

28. On July 28, 2021, law enforcement officers arrested SMITH when he arrived at the Red Robin located at 11500 Midlothian Turnpike #428, Richmond, Virginia 23235, in the Eastern District of Virginia, which was the meeting spot arranged during conversations between SMITH and the OCE. Officers took SMITH into custody as he approached the business adjacent to the designated meeting spot, where he indicated he would wait until the designated meeting time. SMITH drove to the location in the VEHICLE. On SMITH's person at the time of the arrest was an Alabama driver's license. SMITH stated he had traveled to the designated meeting location from his residence in Alabama. Following SMITH's arrest, the VEHICLE was secured and towed to the FBI Richmond Field Office located at 1970 E Parham Road, Richmond, Virginia 23228.

29. During a custodial interview, SMITH admitted to talking online with another female individual from Colorado. The conversation included engaging in sex acts with children, as well as different forms of abuse to include the use of electronic shock collars. SMITH stated he is no longer engaged in conversation with the female individual from Colorado, and that he planned to contact law enforcement if she reached out to him again. Additionally, SMITH admitted to bringing a bag of sex toys to include vibrators and dildos with him to Richmond, Virginia. He stated the bag is located in the VEHICLE. SMITH indicated he is the outright owner of the VEHICLE and that he does not make any payments on it.

CONCLUSION

30. Based on the forgoing, I submit that this affidavit supports probable cause for a warrant to search the VEHICLE described in Attachment A for evidence and instrumentalities of violations of 18 U.S.C. § 2422(b) and 18 U.S.C. § 2423(b) as further described it Attachment B.

Respectfully Submitted,

Matthew Marasco
Special Agent
FBI Richmond Field Office

Reviewed and approved:

MICHAEL MOORE

Digitally signed by MICHAEL MOORE
Date: 2021.08.05 17:57:06 -04'00'

Michael C. Moore
Assistant United States Attorney

Subscribed and sworn to in accordance with Fed. R. Crim. P. 41 by telephone on August 6, 2021

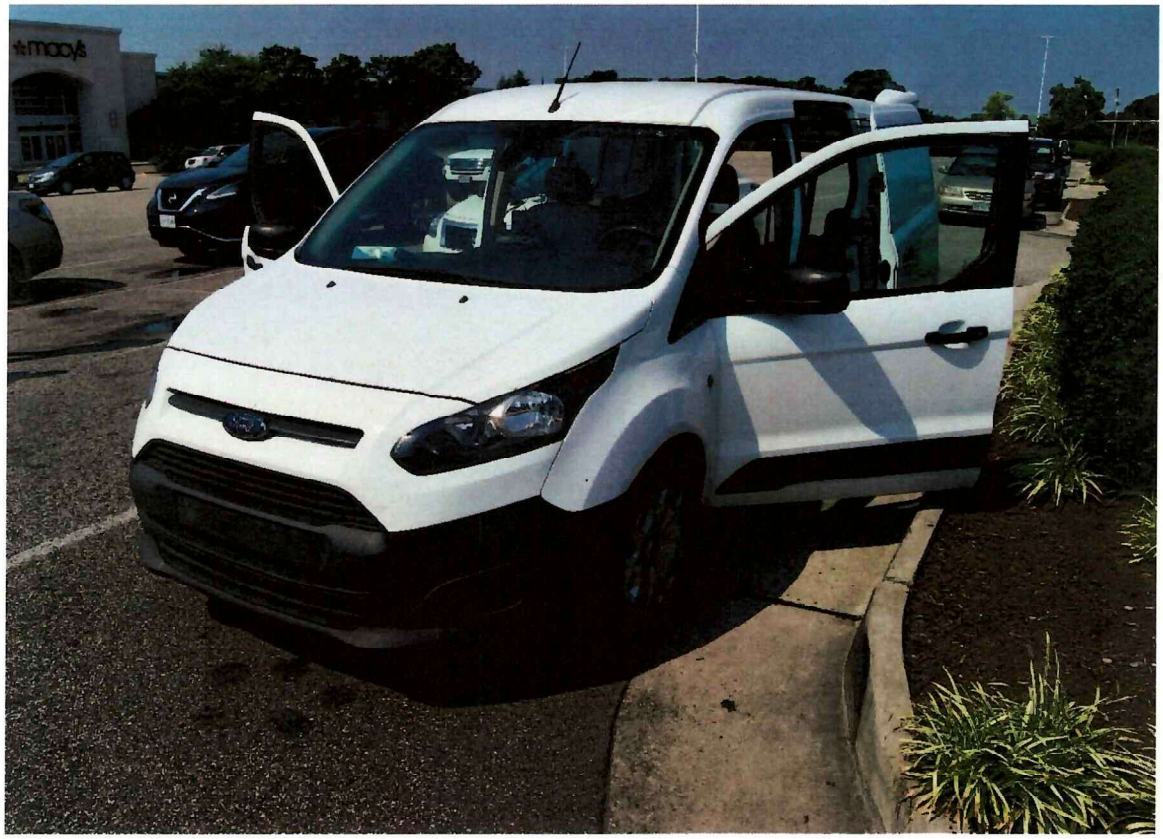
/s/

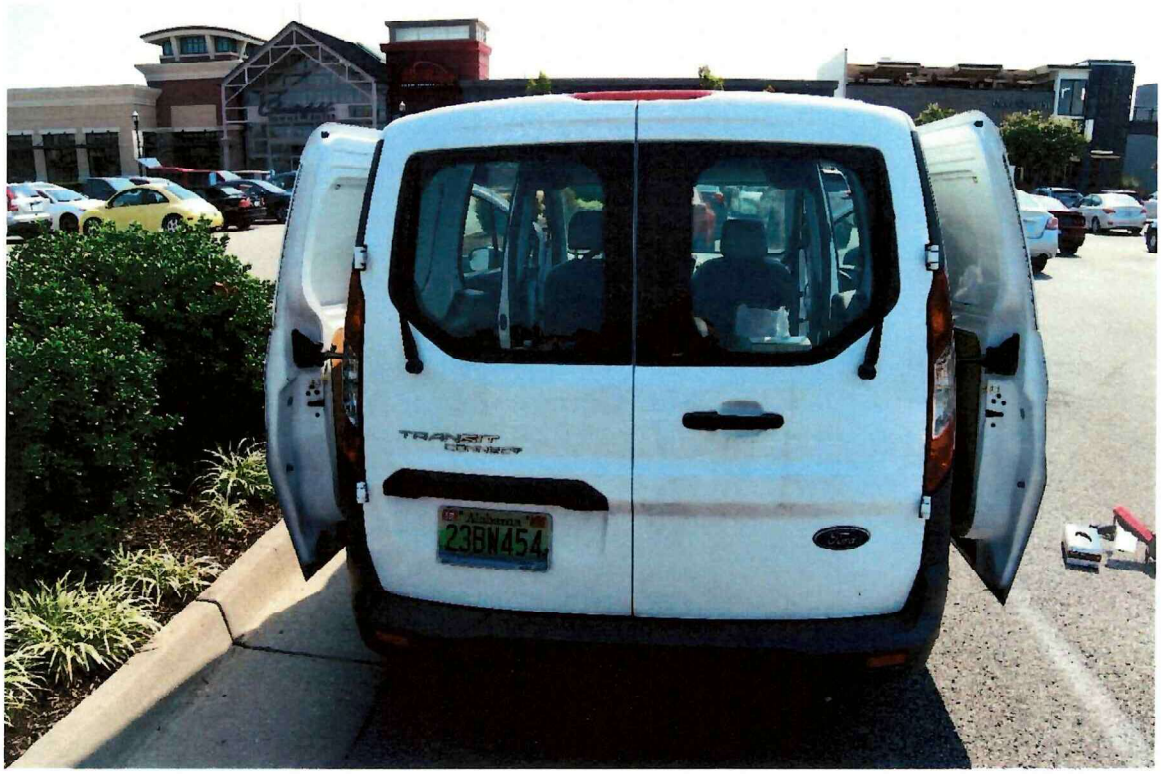
Elizabeth W. Hanes
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to the VEHICLE described as a 2018 Ford Transit Connect 4DR XLT, VIN NM0LS7E79J1368515, located at the FBI Richmond Field Office, 1970 E Parham Road, Richmond, Virginia 23228 (see photographs of the VEHICLE attached below).




TRANSIT
23BN454

ATTACHMENT B

Particular Things to be Seized

1. Fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2422(b), Attempted Coercion and Enticement of a Minor, and 18 U.S.C. § 2423(b), Travel with Intent to Engage in Illicit Sexual Conduct, including:

   a. Any conversations or correspondence regarding the crimes reference above;

   b. Any and all visual depictions of minors, whether or not they are sexually explicit;

   c. Any and all address books, names and lists of names and addresses of minors;

   d. Any and all contracts, diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors; and

   e. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

2. Computers, electronic devices, GPS, or storage media used as a means to commit the violations described above or containing the evidence described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTERs"):

   a. Evidence of violations of 18 U.S.C. § 2422(b) and 18 U.S.C. § 2423(b);

   b. Evidence of who used, owned, or controlled the COMPUTERs at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;

   c. Evidence of software that would allow others to control the COMPUTERs, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   d. Evidence of the lack of such malicious software;

   e. Evidence of the attachment to the COMPUTERs of other storage devices or similar containers for electronic evidence;

   f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTERs.

g. Evidence of the times the COMPUTERs were used;

h. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTERs;

i. Documentation and manuals that may be necessary to access the COMPUTERs or to conduct a forensic examination of the COMPUTERs;

j. Records of or information about Internet Protocol addresses used by the COMPUTERs;

k. Records of, or information about, the COMPUTERs' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

l. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence,

fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

The Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the Court that the imaging process of digital evidence is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the property's owner or his counsel informing the owner that the forensic examination of evidence seized from him has begun. Such notice to the owner and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the owner or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the owner if he is charged. Rather, the sole purpose of this notice is to notify the owner that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the

communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.